TCCネット
接続・設定マニュアル
（琴浦・北栄版）

インターネットをご利用になる前に

Windows 10／8.1 (8) ／ 7 ／ Vista
&
Mac OS X
版

＜目次＞

改訂版・・・（2015年4月）

■ はじめに <必ずお読みください>

ここでは、TCCネットをご使用いただくために必要な情報についてご案内します。

●ご準備いただくもの

TCC ユーザー登録証

発行日	2013/5/1
加入者コード	00000001
加入者名	鳥中　太郎

認証情報

認証ID	abcd1234
認証パスワード	abcd1234
固定IPアドレス	

メール情報

アカウント	tcc12345@mail7.torichu.ne.jp
パスワード	abcd1234
アドレス	tcc12345@mail7.torichu.ne.jp

サーバー情報

メールサーバー(受信)	mail7.torichu.ne.jp
メールサーバー(SMTP)	mail7.torichu.ne.jp
Webサーバー	www7.torichu.ne.jp
DNSサーバー(優先)	XXX.XXX.XXX.XXX
DNSサーバー(代替)	XXX.XXX.XXX.XXX

鳥取中央有線放送株式会社

同封のTCCユーザー登録証	ブロードバンドルーター（BBルーター）	ご利用端末
TCCネットに接続するために必要な情報が記載されております。	お客様のご利用形態（無線使用等）に合わせて電器店等でご準備願います。	パソコンやスマートフォン等インターネットに接続するための端末。

● TCCネット接続方式について

TCCネットでは『PPPoE』とよばれる**認証ID・認証パスワード**を利用する方式でインターネットに接続します。

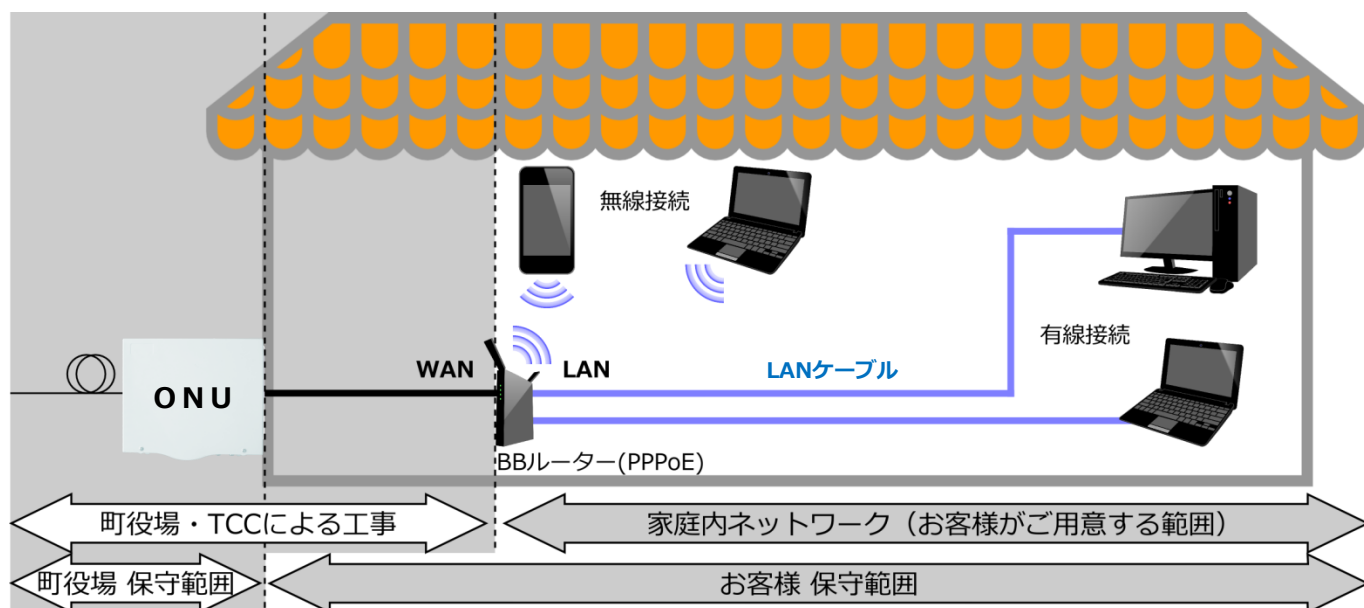
認証ID・認証パスワードは『**TCC ユーザー登録証**』に**認証情報**として記載されておりますのでご確認ください。

TCC　ユーザー登録証

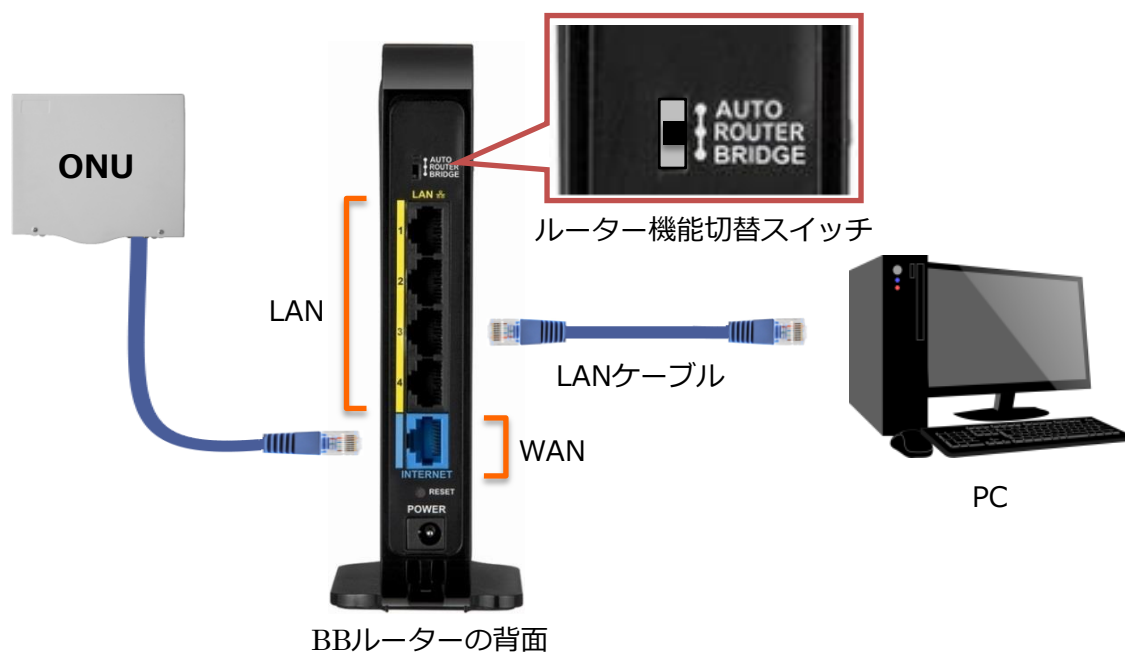
発行日	2015/4/1
加入者コード	00000001
加入者名	鳥中　太郎

認証情報

認証ID	(エー・ビー・シー・ディー・1・2・3・4) abcd1234
認証パスワード	(イー・エフ・ジー・エイチ・5・6・7・8) efgh5678
固定IPアドレス	

● 宅内接続イメージ図

ONUとBBルーターの接続例

1．家の外壁に設置してある”**ONU**”から宅内に引きこまれているLANケーブルをルーターの”**WAN**”ポートへ接続します。（ルーターの機種によっては”**Internet**”と表記してあります）
2．ルーターの”**LAN**”ポートとお使いのパソコンを市販（付属）のLANケーブルで接続します。

※ルーター機能切替スイッチがある場合、”**ROUTER**”側へ切替え、ルーター機能を有効にしてください。（ご利用の機器によって表示が異なる場合があります。詳しくはルーター付属の取扱説明書をご確認ください）

BBルーターの背面

※BBルーターへのPPPoE認証設定が完了するとTCCネットへの接続が可能となります。

BBルーターの設定方法については、BBルーター付属の取扱説明書をご覧になるか、BBルーター製造元のコールセンター、または購入店までお問合わせください。
また、無線接続設定等家庭内ネットワークにつきましては、お客様の責任で構築してください。

設定完了後もTCCネットへ接続できない場合、６ページ以降の『ネットワーク設定(TCP/IP)の確認について（OS別）』をご確認ください。

■電子メールのアカウントの設定について

TCCネットでは、個人で電子メールを利用したり、TCCからの重要なお知らせを通知する為に電子メールを用意しています。
電子メールソフトの設定にはTCCのホームページ、およびメールソフトのホームページの内容を参考にしてください。

URL： http://www.torichu.ne.jp

●メール保存容量

標準でのメール保存容量は 50MB です。
メール保存容量の追加をご希望の方は、有料オプションの「メール保存容量追加」をお申込みください。

●メールソフト設定値の概要

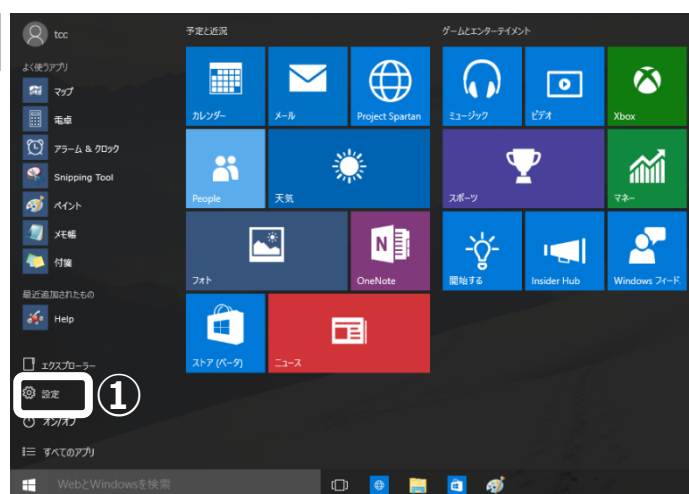
	琴浦エリアの方	**北栄エリアの方**
受信サーバー名	**mx1.tcbnet.ne.jp**	**mail○.torichu.ne.jp** ※○には数字が入ります。ユーザー登録証をご確認ください。
受信サーバーポート番号	**110**	
送信サーバー名	**mx1.tcbnet.ne.jp**	**mail○.torichu.ne.jp** ※○には数字が入ります。ユーザー登録証をご確認ください。
送信サーバーポート番号	**587**	
送信メールサーバー認証	**「このサーバーは認証が必要」**を選択	
送信メールサーバー認証設定	**「受信メールサーバーと同じ設定を使用する」**を選択	
ユーザー名	**アカウント** ※メールアドレスの **「@」より左側の文字列を入力** 例： **tcc1234**@mx1.tcbnet.ne.jp の**tcc1234**部分	**アカウント** **※メールアドレス全体を入力** 例： **tcc1234@mail○.torichu.ne.jp** の全体
パスワード	**パスワード** （ユーザー登録証をご確認ください。）	

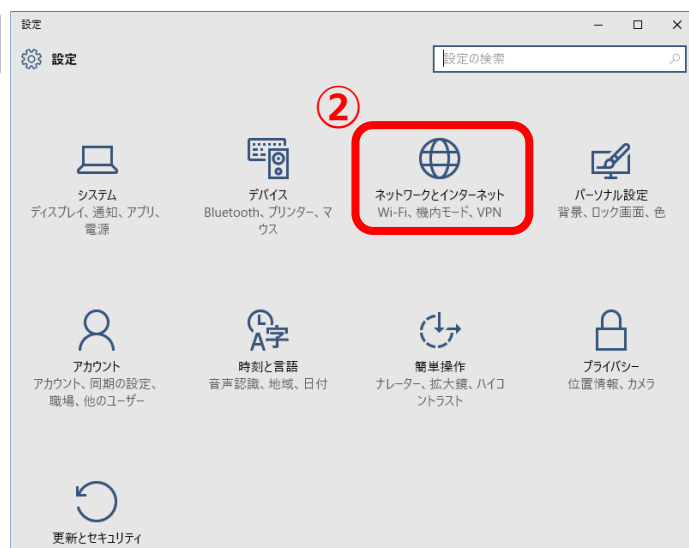
■ネットワーク設定(TCP/IP)の確認について（OS別）

ここでは、OS別に有線接続の場合の設定確認方法についてご案内します。

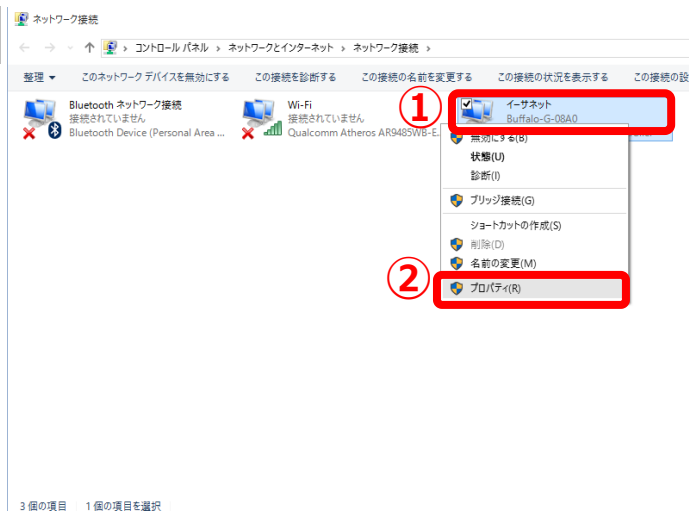
● ≪ Windows 10≫ の場合

1.［設定］を開く

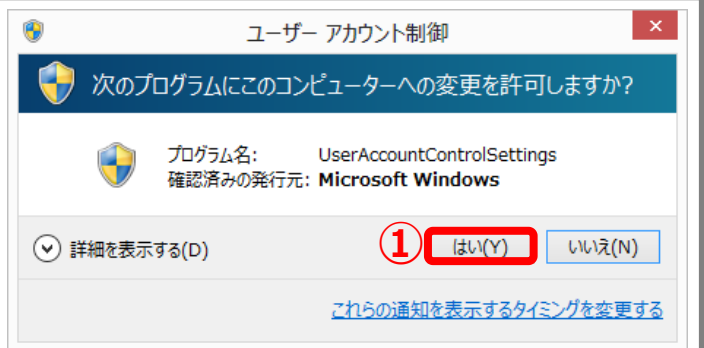
［デスクトップ］画面左下のスタートボタン をクリックし、スタートメニューを表示させ［設定］をクリックします（①）。

2.［ネットワークとインターネット］を開く

［設定］画面が開きます。
［ネットワークとインターネット］を選択します（②）。

3.［ネットワーク接続］を開く

［ネットワークとインターネット］が開きます。
［イーサネット］の中にある、［アダプターの設定の変更］を選択します。（③）。

4.［イーサネットのプロパティ］を開く

［ネットワーク接続］が開きます。
［イーサネット］アイコンを右クリックし（①）、表示されたメニューの［プロパティ］を選択します（②）。

参考

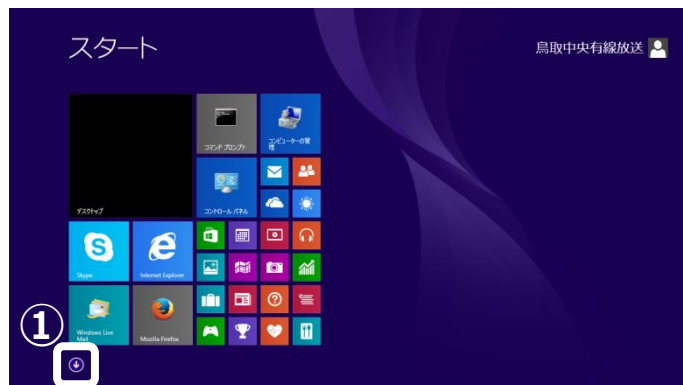
［ユーザーアカウント制御］が　表示された場合、［はい］を選択してください（①）。

※ここから先は各WindowsOS共通の操作となります。

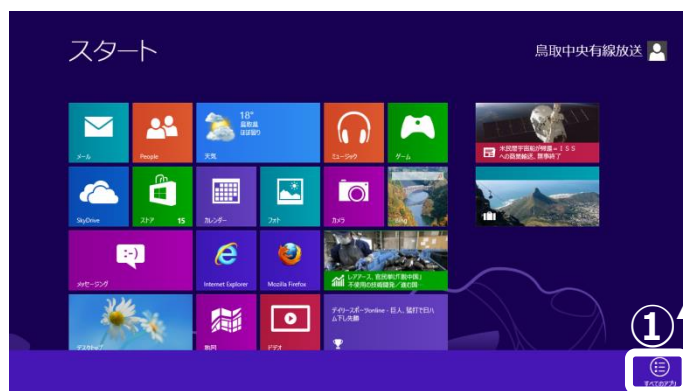
１６ページへお進みください。

●≪ Windows 8.1（Windows 8）≫ の場合

1.［全てのアプリ］を開く

Windows 8.1

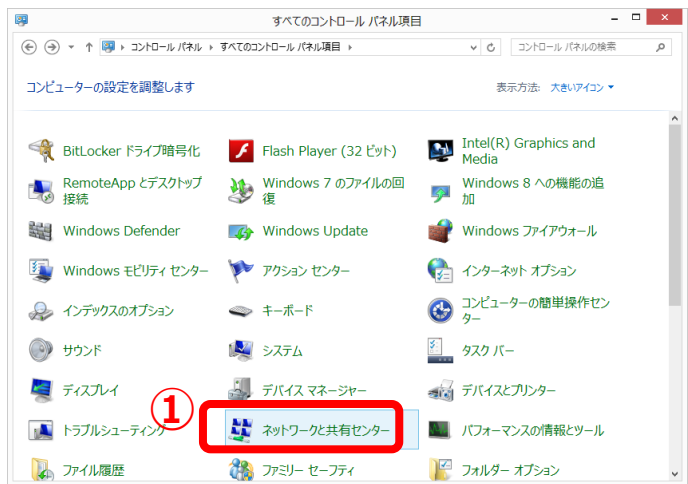
［スタート］画面左下の をクリックします（①）。

Windows 8

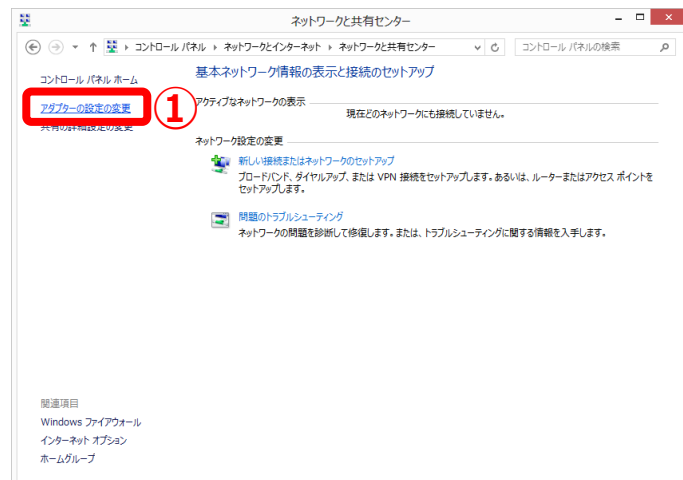
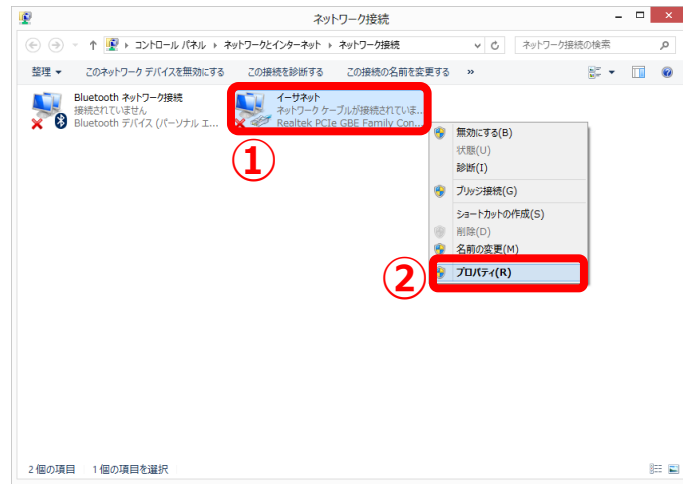
［スタート］画面で**右クリック**し、画面右下に［全てのアプリ］を表示させ、クリックします（①'）。

2.［コントロールパネル］を開く

［全てのアプリ］が開きます。
［コントロールパネル］を選択します（①）。

3.［ネットワークと共有センター］を開く

［コントロールパネル］が開きます。
［ネットワークとインターネット］の中にある、
［ネットワークの状態とタスクの表示］を選択
します。（①）。

参考
アイコン表示の場合、［ネットワークと
共有センター］を選択します（①）。

4.［ネットワーク接続］を開く

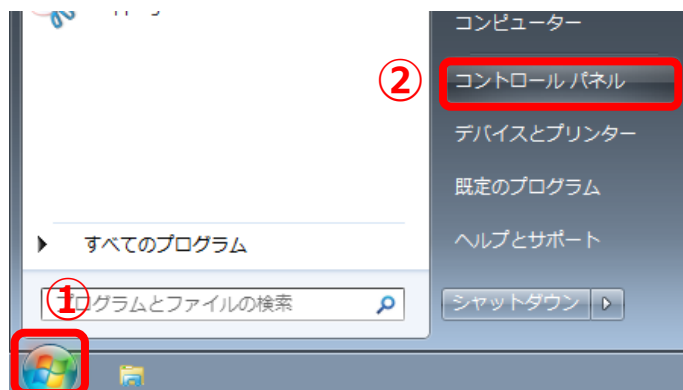
［ネットワークと共有センター］が開きます。
左側メニューの［アダプターの設定変更］を選択
します（①）。

5.［イーサネットのプロパティ］を開く

［ネットワーク接続］が開きます。
［イーサネット］アイコンを右クリックし（①）、表示されたメニューの［プロパティ］を選択します（②）。

参考
［ユーザーアカウント制御］が　表示された場合、［はい］を選択してください（①）。

※ここから先は各WindowsOS共通の操作となります。

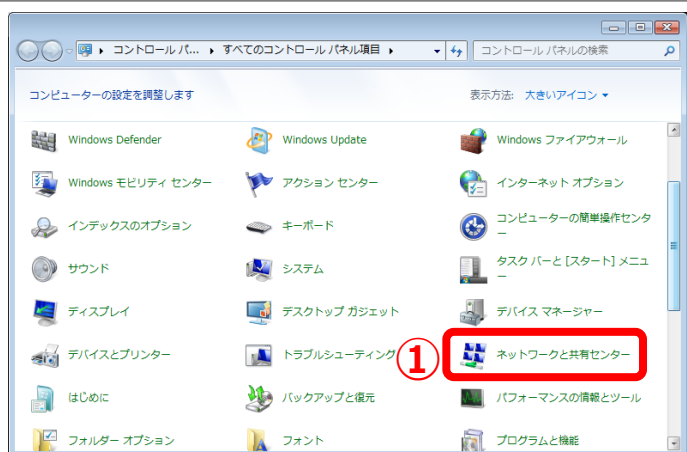
１６ページへお進みください。

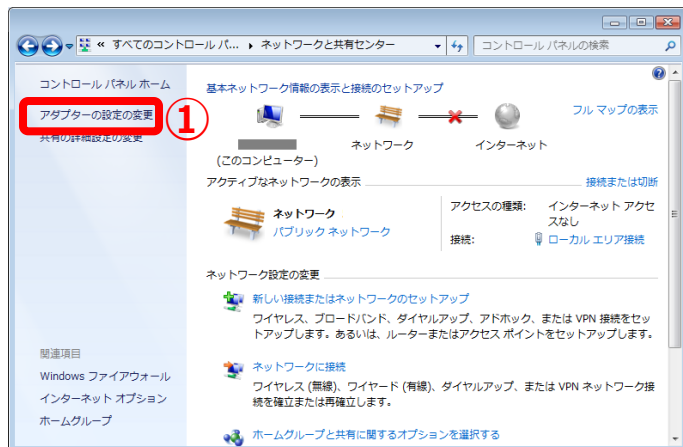
●≪ Windows 7 ≫ の場合

1.［コントロールパネル］を開く

パソコン画面左下にある［スタート］（①）から、
［コントロールパネル］を選択します（②）。

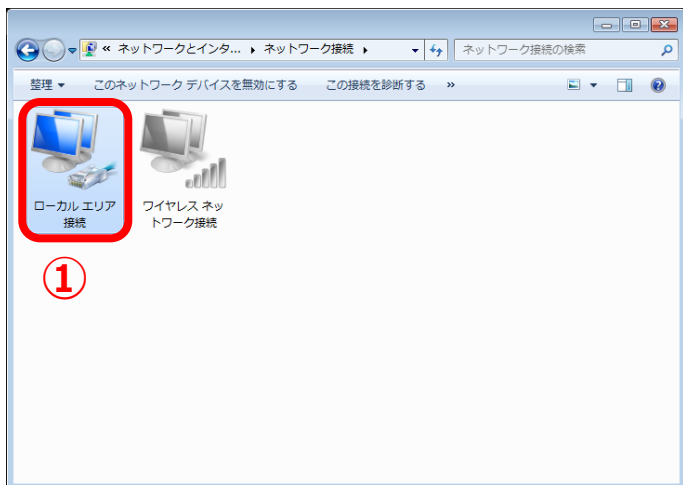
2.［ネットワークと共有センター］を開く

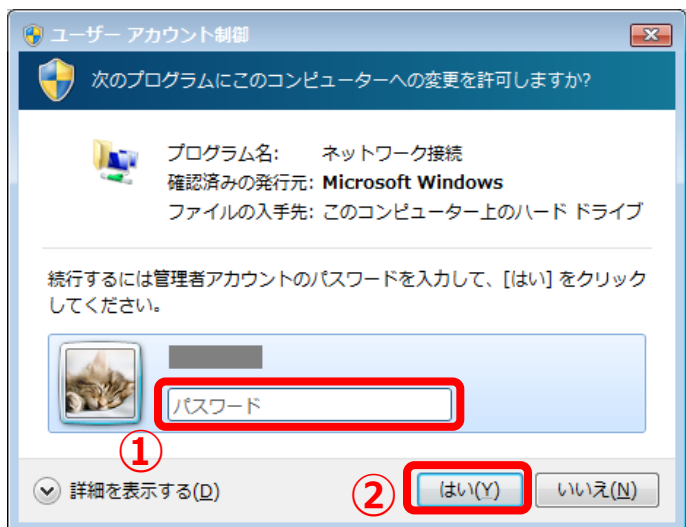
［コントロールパネル］が開きます。
［ネットワークとインターネット］の中の
［ネットワークの状態とタスクの表示］を選択
します（①）。

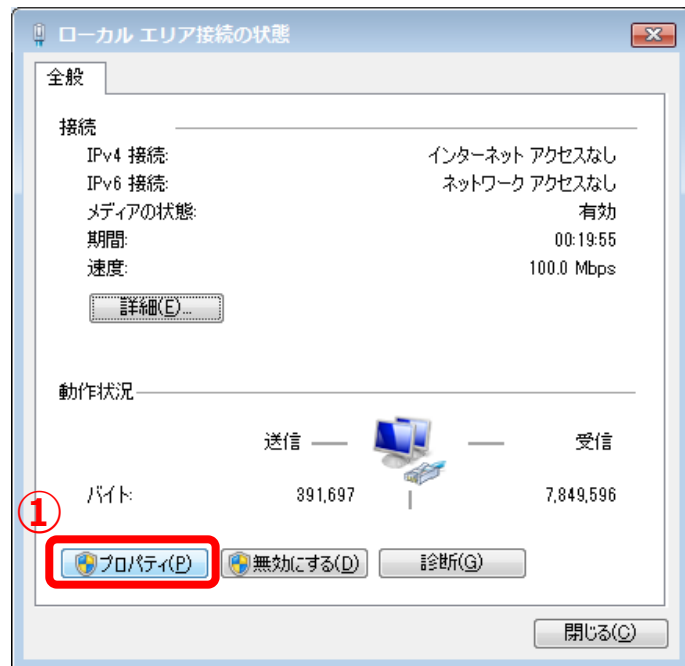
参考
アイコン表示の場合、［ネットワークと
共有センター］を選択します（①）。

3.［ネットワーク接続の管理］を開く

［ネットワークと共有センター］が開きます。
左側メニューの［アダプターの設定の変更］を選択します（①）。

4.［ローカルエリア接続の状態］を開く

［ネットワーク接続］が開きます。
［ローカルエリア接続］のアイコンをダブルクリックします（①）。

参考

［ユーザーアカウント制御］が表示された場合、管理者アカウントのパスワードを入力し（①）、［はい］を選択してください（②）。

（管理者アカウントにパスワードを設定していない場合、パスワードの入力は必要ありません。）

5.［ローカルエリア接続のプロパティ］を開く

［ローカルエリア接続の状態］が開きます。
画面下部の［プロパティ］を選択します（①）。

※ここから先は各WindowsOS共通の操作となります。

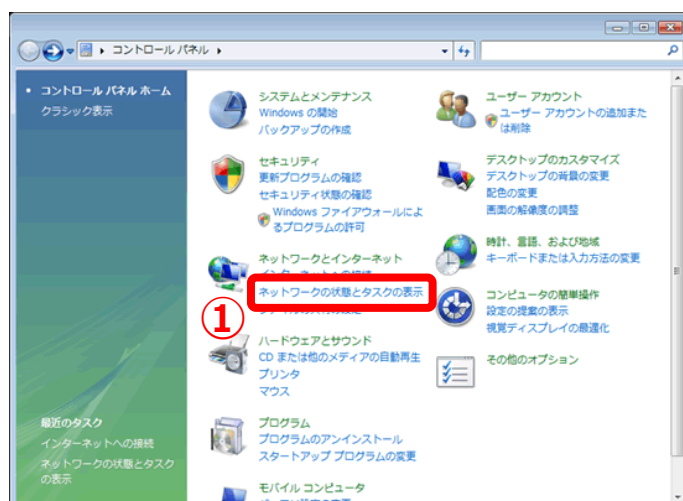
１６ページへお進みください。

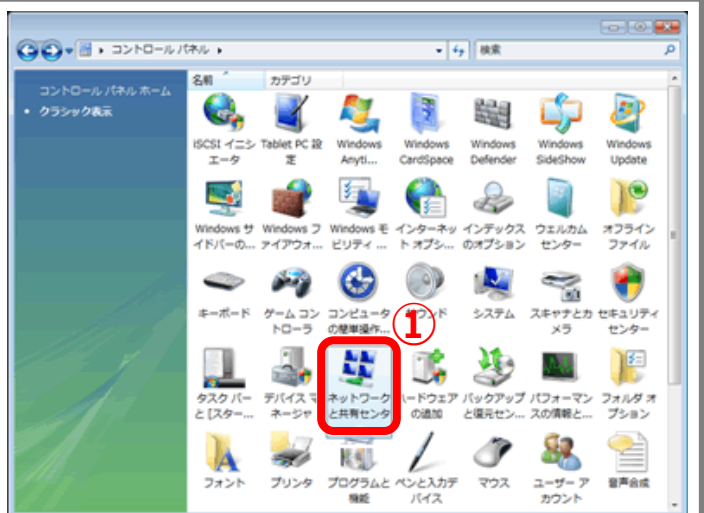
● ≪ Windows Vista ≫ の場合

1.［コントロールパネル］を開く

パソコン画面左下にある［スタート］（①）から、［コントロールパネル］を選択します（②）。

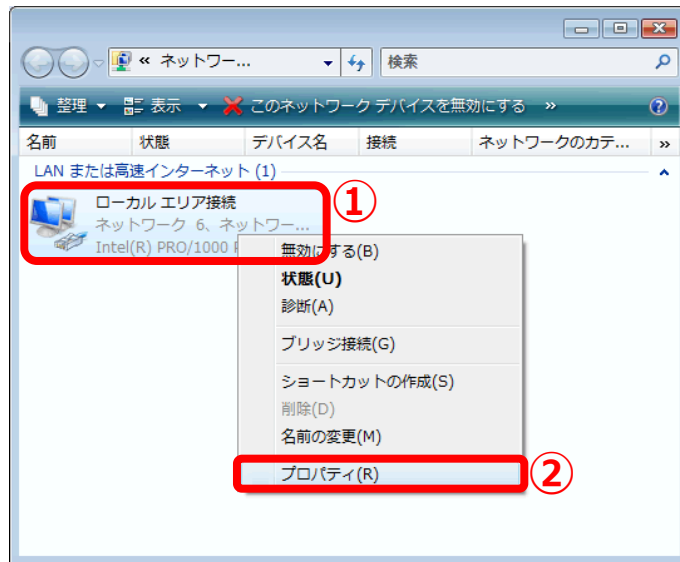
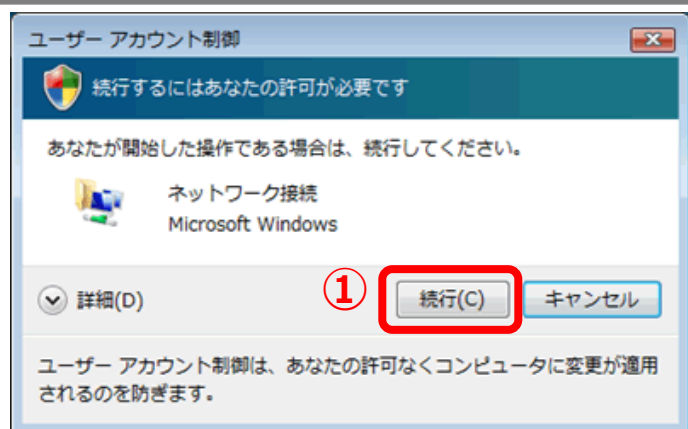
2.［ネットワークと共有センター］を開く

［コントロールパネル］が開きます。
［ネットワークとインターネット］の中の［ネットワークの状態とタスクの表示］を選択します（①）。

参考

クラシック表示の場合、［ネットワークと共有センター］を選択します（①）。

3.［ネットワーク接続の管理］を開く

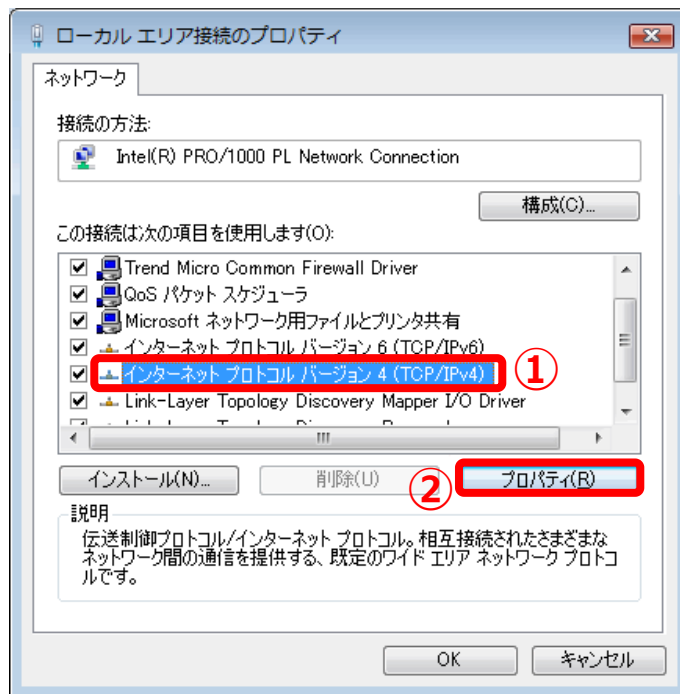
［ネットワークと共有センター］が開きます。
左側メニューの［ネットワーク接続の管理］を選択します（①）。

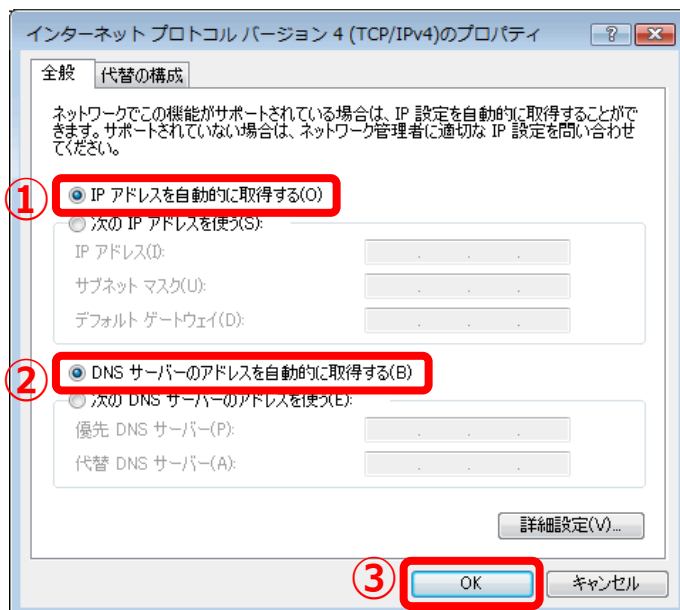
4.［ローカルエリア接続のプロパティ］を開く

［ネットワーク接続の管理］が開きます。
［ローカルエリア接続］アイコンを右クリックし（①）、表示されたメニューの［プロパティ］を選択します（②）。

参考
［ユーザーアカウント制御］が表示された場合、［続行］を選択してください（①）。

次ページからは各WindowsOS共通の操作となります。

●≪ Windows 共通部分 ≫

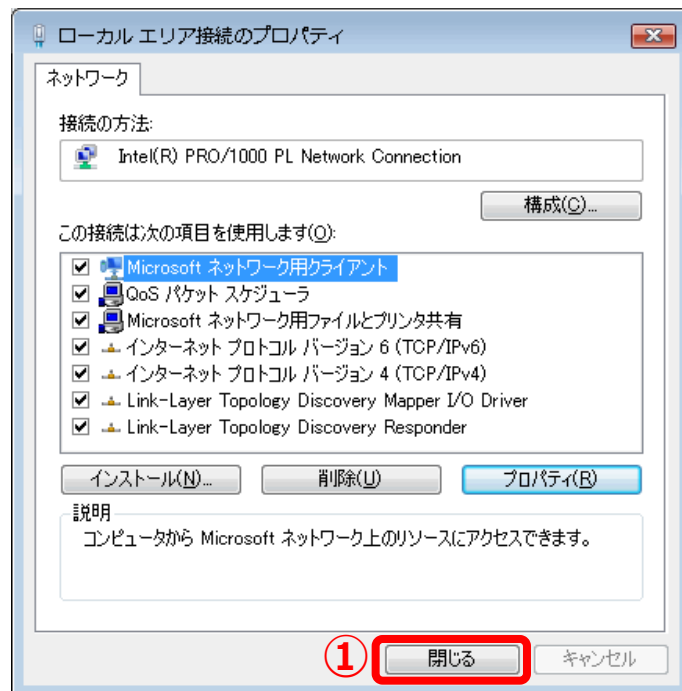
1.［インターネット プロトコル バージョン 4 (TCP/IPv4) のプロパティ］を開く

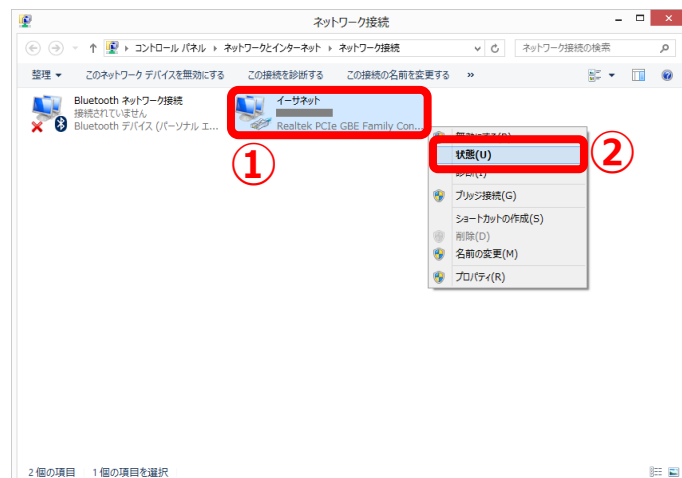
［イーサネット（ローカルエリア接続）のプロパティ］が開きます。
［インターネット プロトコル バージョン 4 (TCP/IPv4)］を選択し（①）、［プロパティ］を選択します（②）。

2.［TCP/IPv4］と［DNSサーバー］の設定を確認する

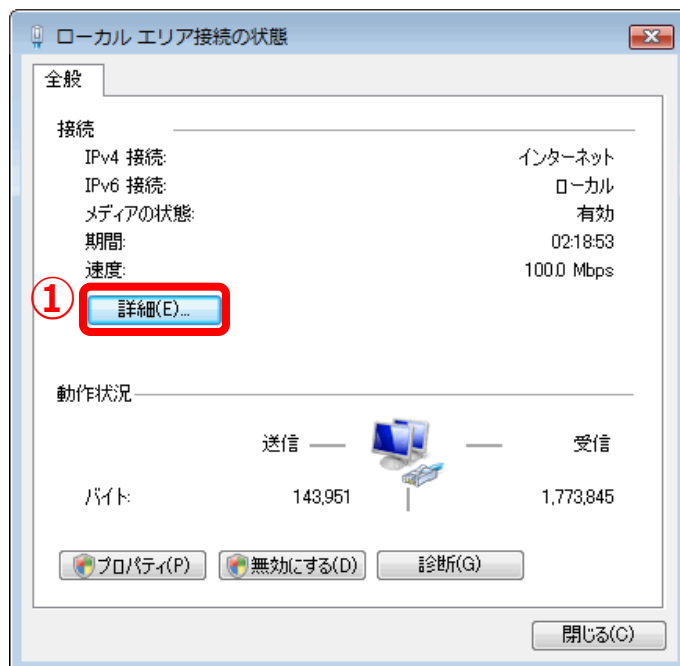
［インターネット プロトコル バージョン 4 (TCP/IPv4) のプロパティ］が開きます。
［IPアドレスを自動取得する］にチェックが入っていることを確認します（①）。
［DNSサーバのアドレスを自動的に取得する］にチェックが入っていることを確認します（②）。
確認後、下方の［OK］を選択します（③）。

参考
ローカルエリアネットワーク設定では［IPアドレス］、ならびに［DNSサーバー］は「**自動取得**」でお使いください。

（以上でネットワーク設定は完了です。以降はネットワーク設定の確認方法です。）

3.［ネットワーク接続の管理］に戻る

［イーサネット（ローカルエリア接続）のプロパティ］に戻ります。
下方の［閉じる］を選択します（ ① ）。

4.［ローカルエリア接続の状態］を開く

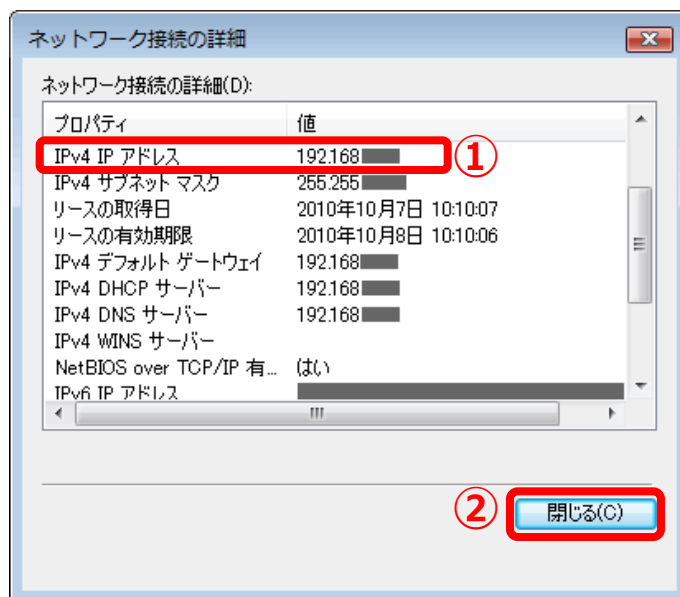
［ネットワーク接続］に戻ります。
［イーサネット（ローカルエリア接続）］アイコンを右クリックし（①）、表示されたメニューの［状態］を選択します（②）。

5.［ネットワーク接続の詳細］を開く

［イーサネット（ローカルエリア接続）の状態］が開きます。
［詳細］を選択します（①）。

6.［ネットワーク接続の詳細］を確認する

［ネットワーク接続の詳細］が開きます。
［IPv4 IPアドレス］が下記のような値になっていることを確認する（①）。

・BBルーター利用の場合
［ 192. 168. *. ***※ ］**

※ ***は数字

確認後、下方の［閉じる］を選択します。

<注意>
「0. 0. 0. 0」 または「169. *. ***. ***」で始まるIPアドレスが表示された場合、IPアドレスが正常に取得されていません。**
接続状態、およびパソコンの状態をご確認ください。

パソコンが取得する［IPv4 アドレス］の値は、BBルーターの『DHCPサーバー設定』に依存します。
詳しくはルーター付属の取扱説明書、またはルーター製造元のコールセンターまでお問合わせください。

● ≪ Mac OS X ≫ の場合

1.［システム環境設定］を開く

［アップルメニュー］を選択し（①）、その中の［システム環境設定］を選択します（②）。

参考

Dockの中からも［システム環境設定］を表示できます（①）。

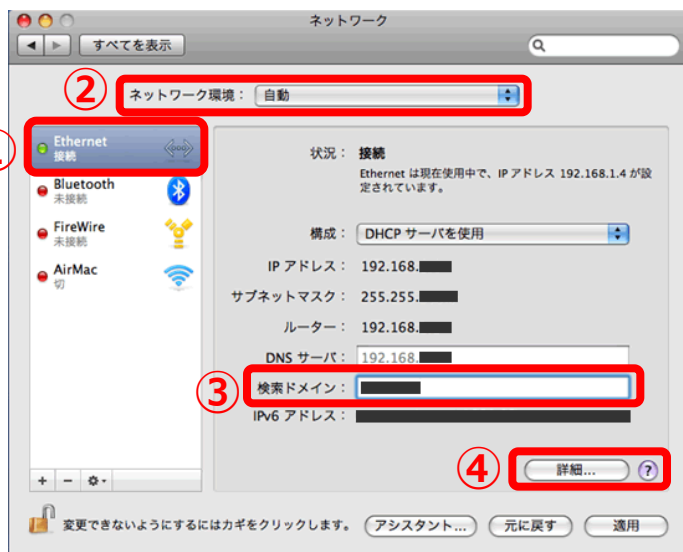
2.［ネットワーク］を開く

［システム環境設定］が開きます。
［ネットワーク］を選択します（①）。

3.［Ethernetの詳細］を開く

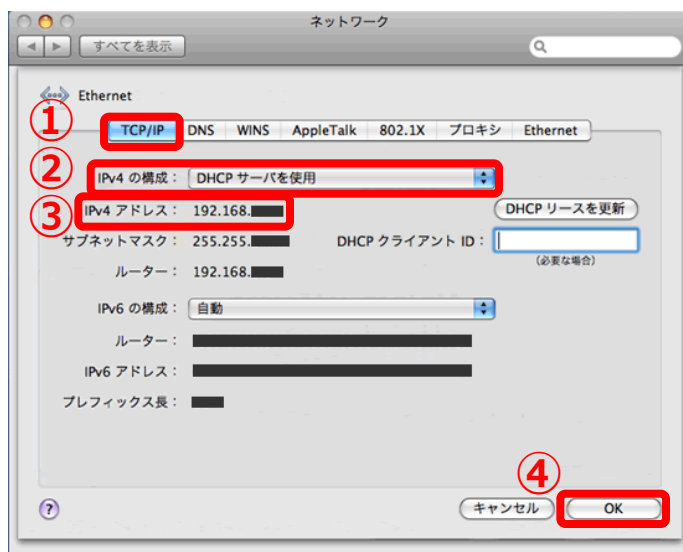
［ネットワーク］が開きます。
左側メニューの中の［Ethernet］が選択されていることを確認します（①）。
［ネットワーク環境］を［自動］に設定し（②）、［検索ドメイン］に下記を設定します（③）。

・検索ドメイン　　　［ torichu.ne.jp ］

［詳細］を選択します（④）。

4.［ネットワーク接続］を開く

［Ethernetの詳細］が開きます。
［TCP/IP］タブを選択します（①）。
［IPv4の構成］を［DHCPサーバを使用］に選択し（②）、［IPv4 アドレス］が下記のような値になっていることを確認する（③）。

・BBルーター利用の場合
［ 192.168.*.***※ ］**

確認後、［OK］を選択します（④）。

<注意>
「0.0.0.0」または「169.*.***.***」で始まるIPアドレスが表示された場合、IPアドレスが正常に取得されていません。**
接続状態、およびパソコンの状態をご確認ください。

パソコンが取得する［IPv4 アドレス］の値は、BBルーターの『DHCPサーバー設定』に依存します。
詳しくはルーター付属の取扱説明書、またはルーター製造元のコールセンターまでお問合わせください。

■ ホームページ開設について

TCCネットでは、個人がホームページを開設をするためのwebサーバーを用意しています。お客様自身でホームページを開設することが可能です。
ホームページのデーター作成、webサーバーへのデーターのアップロード、および内容変更はお客様自身で行ってください。

● web保存容量

web保存容量は 50MB まで無料でご利用頂けます。
web保存容量の追加をご希望の方は、有料オプションの「web保存容量追加」をお申込みください。

● アップロード方法

TCCのwebサーバーへFTPを行う場合の基本事項は下記の通りです。

	琴浦エリアの方	北栄エリアの方
ホスト名 **（webサーバー）**	**hp1.tcbnet.ne.jp**	**www○.torichu.ne.jp** ※○には数字が入ります。ユーザー登録証をご確認ください。
初期ディレクトリ	**public_html**	
ログイン名	**アカウント** ※**「@」より左側**の文字列を入力 例： **tcc1234**@mx1.tcbnet.ne.jp の**tcc1234**部分	**アカウント** ※**アカウント全体**を入力 例： **tcc1234@www○.torichu.ne.jp** の全体
パスワード	**パスワード** （ユーザー登録証をご確認ください。）	
URL	**http://hp1.tcbnet.ne.jp/~アカウント/**	**http://www○.torichu.ne.jp/~アカウント/** ※○には数字が入ります。ユーザー登録証をご確認ください。

※ public_html フォルダにhtmlファイルなどをアップロードしてください。
※ トップページは "index.html" というファイル名にしてください。

■無料オプションについて

TCCネットでは、お客様のご利用環境に合わせた、無料のオプションを用意しています。（ご利用には一部TCCのホームページからの登録が必要です。）

URL：http://www.torichu.ne.jp

● ｉ－フィルター

犯罪サイト、アダルトサイトなど、有害情報を掲示しているwebサイトを閲覧したくない、又は閲覧させたくない場合にwebサイトの表示をブロックします。webサイトを閲覧される方の年齢や、ポリシーに応じて、ブロックするサイトの設定を変えることができます。
設定は全てパスワードで管理しますので、フィルタリングの解除や設定の変更がパソコンの管理者の許可なくできないように保護されます。

●無料スパムカット

スパムカットは、スパムメール（迷惑メール）を自動的に判別、あるいは設定した条件のものを、サーバ側の専用フォルダ（ごみ箱）に自動的に振り分けます。
これにより、不要な迷惑メールを自分のパソコンに取り込む必要がなくなります。
振り分けられた迷惑メールについては、サーバ側にて一定期間保存され、保存期間を過ぎたものは自動的に削除されます。
フィルタリングの条件は、事前に登録されているデータベースを参照し、サーバ側で振り分けます。
またそれ以外にも、受信拒否アドレス、受信許可アドレスの設定が可能となります。
ごみ箱に、振り分けられたメールは転送されません。

●無料ウェブメール

無料ウェブメールサービスは、パソコン上のwebブラウザや、携帯電話のweb機能（i-modeなど）から、TCCの『受信サーバー』に入っているメールの閲覧、送受信、転送などが可能になります。
外出先からでも、メールのチェックが可能になります。また、webメールで受信したメールは、『受信サーバー』に残っていますので、後で自宅のパソコンのメールソフトから閲覧することができます。

（バージョンアップなど）都合により、記載の内容と変わることがあります。
詳しくはTCCのホームページ（ http://www.torichu.ne.jp）をご覧ください。

インターネットサービスの利用に関するガイドライン

はじめに
鳥取中央有線放送株式会社(以下「当社」と言います)では、さまざまなインターネットサービス(以下「本サービス」と言います)を提供しています。本サービスは、多くのユーザーによって共有されています。さらに、本サービスを利用して接続するインターネット上には、当社のユーザー以外にも世界中に存在する不特定多数のユーザーが存在しています。それぞれのユーザーは、インターネットを利用して、情報を共有したり、他のユーザーと通信をしたりなどの様々な恩恵を受けます。その一方で、他のユーザーの権利を侵害しない、迷惑をかけないなどの義務や責任を負うことになります。
このサービスの利用に関するガイドライン(以下「本ガイドライン」と言います)では本サービス(開始しているサービスに限る)のご利用にあたり、守っていただきたい規則やガイドラインについて説明しています。本ガイドラインの内容をご一読の上、定められた規則を遵守していただきますようお願いします。
本ガイドライン、および契約約款に規定されている規則やガイドラインを破り、当社の警告を無視して他のユーザーに迷惑となる行為を続けた場合、契約約款の規定に基づき、サービスの停止を行う場合があります。

1.セキュリティについて

セキュリティとは、インターネットを安心して利用するために注意を払うべき安全対策のことをいいます。 インターネットは誰にでも開かれている自由な社会ですが、まだ秩序が整っていない発展途上の場という側面も持っています。自分の身は自分で守らなくてはなりません。したがって、侵入者や違法な行為を行う人々を日頃から十分認識しておくことが大切です。

1.1 アカウント情報、およびパスワード管理

電子メールやショッピングサイト等インターネット上の取引を行う場合、自分のユーザーアカウントを登録する必要があります。ユーザーアカウントを使用するためには、与えられたユーザー名を使用して、本人性の確認のためにユーザー認証を受けなければなりません。ユーザー認証の際には、自分がそのユーザー名の正式な所有者であることを証明するために、パスワードを入力しなければなりません。

1.1.1 パスワード管理上の注意事項

自分の氏名、生年月日、電話番号など、容易に類推できるパスワードでは、危険から身を守るのには十分とはいえません。ショッピングサイト等を利用する場合、登録するパスワードをわかりにくいように工夫してください。また、当社では、無作為に作成された文字列を電子メールアカウントのパスワードとして発行しております。他人に自分のユーザーアカウントを使用されないよう、パスワードの管理には十分にご注意ください。

1.1.2 パスワード管理を怠ると

他人に自分のユーザーアカウントを使用されてしまうと、以下のような危険にさらされます。

- 本来は使用権限が与えられていないユーザーがネットワークに接続できるようになる。
- 自分の電子メールアドレスに届いたメールの内容が他人に読まれる。
- ショッピングサイトなどで、商品の購入履歴や住所、電話番号などの個人情報が漏洩することになります。
- ショッピングサイトによっては、会員管理としてカード番号を登録していることがあるため、他人の登録したカードで買い物をされてしまう可能性もあります。

このような、第三者による不正アクセスを防止するためには、各々のユーザーがID 、およびパスワードの管理に常に注意を払ってください。

1.2 プライバシーの遵守

インターネットの世界でも、実社会と同様に、プライバシーは守られなければなりません。特にインターネットでは不特定多数のユーザーが接続する可能性があるため、細心の注意を払って個人情報を管理しなければなりません。

1.2.1 プライバシーの保護

各々のユーザーにとって、最も大切なことは自分や知人の個人情報を不用意に公開しないことです。ホームページを開設し、掲示板やアンケートサイトなどを用意している場合は、収集した情報の管理について、責任があるということを認識しなければなりません。
個人の住所、氏名、電話番号、生年月日などのプライバシーに関わる情報を収集する場合には、万全な情報セキュリティ体制のもとで管理する義務があると言えます。また、複数の人に電子メールを送信する場合、宛先のメールアドレスを送信先すべてに公開してよいか判断する必要があります。

1.2.2 他人のプライバシーを侵害する行為とは

以下のような行為はプライバシーの侵害として問われる可能性があります。

- 開設しているホームページ等で収集した他人の個人情報をインターネット上で公開した。個人情報とは、住所・氏名・電話番号など個人を特定可能とする情報だけでなく、本人に承諾のない電子メールの内容の引用、特定のメールアドレスからのアクセス履歴など、個人情報と関連性のあるデータ情報を含みます。
- 複数の人に電子メールを送信する際に、宛先、またはCC(Carbon Copy)に指定して送信した。この場合、受信者間に面識がない場合、個人が保持するメールアドレスが公開されたことになります。

1.3 ウイルス対策

コンピューターウイルスは、電子メールやホームページ閲覧などによってコンピュータに侵入する特殊なプログラムです。最近はインターネットの普及に伴い、電子メールをプレビューしただけで感染するものや、ホームページを閲覧しただけで感染するものが増えてきています。また、インターネット利用者の増加や常時接続回線が普及してきたことで、ウイルスの拡大が速くなってきています。

1.3.1 コンピューターウイルスに感染しないための対策

当社では、メールウイルスチェックサービスを無料で行っておりますが、これは電子メールによる感染を防止する対策となります。ウイルスの感染経路としては、

- 電子メールの他に・ホームページの閲覧によるインターネットを介した感染
- ネットワークのファイル共有によるネットワークを介した感染
- マイクロソフト社のOfficeアプリケーション(Word、Excel、PowerPoint、Access)のマクロ機能を利用したプログラムの実行による感染

などがあります。このようなコンピューターウイルスに感染しないようにするためには、以下のような対策があります。

- ウイルス対策ソフトを導入し、常に最新のウイルスに対応できるように、インターネットなどでウイルス検知用データを更新しておきます。
- Windows のパソコンをご利用の場合は、マイクロソフト社が無償配布しているWindows の修正プログラムを適用することで、パソコンのセキュリティを強化する対策となります。ウイルス対策ソフトを用いても、残念ながらウイルス対策は万全とはいえません。
- 不審な電子メールを受信した場合は、削除してください。このような電子メールに添付ファイルがある場合は、開かないことが賢明です。
- ファイルのダウンロードを行う際は、配信元が信頼できるサイトであるか確認してください。
- 定期的にデータのバックアップをとっておけば、万一ウイルスに感染しても被害を最小限に抑えることができるでしょう。

1.3.2 コンピューターウイルスに感染してしまうと

コンピューターウイルスに感染しますと、コンピュータが動かなくなったりファイルが壊れたりと、さまざまな障害がでます。また、コンピュータに登録されている電子メールのアドレス帳や過去の送受信履歴を利用して、自動的にウイルス付きの電子メールを送信するものも多く、世界中にウイルスが蔓延する大きな原因となっています。

2.電子メール

当社から提供されている電子メールアドレスを使用して、インターネット上に存在する世界中の人と電子メールをやり取りすることができます。メッセージを送ることもできますし、ちょっとした電子ファイルを添えて送ることもできますが、セキュリティはそれほど高くありません。たくさんのネットワークを経由して届けられることから、送信の途中で紛失したり覗かれたりする危険もあります。

2.1 電子メールご利用において

すぐに配達される電子メールは会話のように気軽に楽しむことができますが、便利である反面、メッセージがどのように相手に受け取られるかなど、電子メールの特性を考慮し、ご利用においては十分に注意しなくてはなりません。電子メール使用時には、以下のようなことを考慮してください。

- インターネット上のメールは安全ではないものと考えておかなければなりません。クレジットカード番号やパスワードなど他人に知られたくない個人情報や非公開情報などは決してメールに含めてはいけません。
- 相手に対して常に寛容であるよう心がけ、人を不愉快にさせるような話や言葉遣いは慎みましょう。

- あなたが送ろうとするメッセージがどれだけ大きいのかを知っておきましょう。容量の大きなメッセージや添付ファイルは、宛先のコンピュータシステムや途中経由するインターネットサーバの故障を誘発する可能性があります。送信しようとしているメッセージや添付ファイルの容量が大きいと思うときは、相手先に確認してから送信しましょう。
- 電子メールでは、絶対にチェーンメールを送ってはいけません。 チェーンメールとは、はっきりと相手を特定しないで伝言を求める電子メール。
- 宛先にメールのアドレスを書く時には、間違いのないよう慎重に入力しましょう。また、個人のアドレスのように見えても、実はあるグループに送られるというアドレスもあります。誰に送ろうとしているのかを知っておきましょう。
- 返事をするときには、cc（Carbon Copy）の宛先に気をつけましょう。メッセージが1対1のやりとりになるときには、他人を巻き込み続けてはいけません。
- 不愉快な内容の電子メールを受取ったら、相手にしないようにしましょう。また、挑発的な言葉を投げかけられても応じてはいけません。常に冷静に対応するよう心がけましょう。
- 電子メールの内容を他の場所に転載したりすると著作権の侵害にあたる場合もあります。また、あなた以外の人に知られることによって本人の名誉が傷つくことや、プライバシーに関する情報が漏れて迷惑をかけるかもしれません。受け取った電子メールを転送したり転載したりする場合には、本人に連絡して承諾を得るのが良いでしょう。私信である電子メールをホームページなどの公開された場所に掲載するときは、ことさら慎重に取り扱うべきです。

2.2 覚えのないメールには要注意

2.2.1 メーリングリスト

加入に際しては、そのメーリングリストが信頼にあたいするものであるかどうか良く検討してください。またリストから除外してもらいたい場合どのようにすれば良いのかを事前に確認してから加入しましょう。また知人が勝手に登録していたというような例もあるので、自分が登録した覚えがなければその旨連絡して登録を抹消してもらいましょう。

2.2.2 ねずみ講

実社会同様、自分が被害者になると同時に加害者になる可能性もあるので、ねずみ講メールかなと思ったら、絶対に転送しないことです。

事例：「住所氏名がリストアップされている5人に500円を送り、リストの一番上を消し、二番目以降を順次繰上げ五番目に自分の住所氏名を載せメールを出来るだけたくさんの人に送れば、数百万の収入がある」

2.2.3 スパムメール

身に覚えのないところから届くダイレクトメールなど自分にとって不要なメールが頻繁に届き、本来の必要なメールを捜すのに大変苦労することになります。このようなメールは、返信などせず無視して削除することが賢明です。このようなメールの受信が永続的に続く場合は、メールアドレスを変更することもひとつの対策となります。

2.2.4 チェーンメール

自分の所で断ち切る勇気を持ちましょう。このようなメールは他人に再送信すると、拡大してメールサーバーに障害を与る恐れや、通信混乱を招く恐れがあるので、決して転送せずに、即刻削除することです。

事例：「幸せのメールという電子メールが届き、5人に送るように指示が書かれていた。」

2.2.5 爆弾メール

一度に大量のメールを送信され、メールBOX 容量がいっぱいとなり、必要なメールが取り出せなくなったりします。加入するプロバイダに連絡し、自分のメールボックスにあるメールの削除を依頼するなどの対処となります。お使いのメールソフトに、特定のメールアドレスからの受信拒否を行う機能があれば、それを使用することも対策のひとつです。

2.2.6 ウイルスメール

知らない人から届いたメールの添付ファイルを開いて、コンピューターウイルスに感染する場合があります。身に覚えのないメールは開かずに削除することが賢明です。少なくとも添付ファイルは安易に開かない（添付ファイルはウイルスが入っている場合がある）ことです。市販のパソコンウイルスチェッカーを導入して、新しく受信したファイル等を開く前に必ずウイルスチェックをすることも対策のひとつです。いずれにしても、重要なファイルやプログラムは、必ずバックアップを取ることが必要です。

3.ホームページ

広い範囲の人々に向かって情報を発信できるホームページは、インターネットの大きな魅力の一つとなっています。当社のホームページサービスやその他インターネットサービスで公開する情報については、個人が発信する情報に責任を持つことになります。

3.1 作成したホームページの内容に責任を持つ

ホームページの掲載内容には、ホームページ開設者個人が責任を持つことになります。 当社は、ユーザーが開設しているホームページの内容について責任を負うことはできません。

3.2 ホームページ公開時の考慮すべき事項

インターネット上で公開されるホームページは、多くの人に閲覧されます。責任を問われることにならないよう、掲載内容には十分な注意を払う必要があります。

3.2.1 著作権侵害をしない

文章や写真、音楽、ソフトウェアなどの著作物には著作権があります。他人のホームページや電子掲示板や雑誌に載っている著作物を、無断で使用してホームページを作成する等、著作権を侵害しないようにしましょう。

3.2.2 誹謗・中傷しない

ホームページ上で人を批判するときには、相手の人格を否定するような過激な書き方をしてはいけません。あまり度が過ぎると、法的な責任を問われる深刻な事態になることがあります。

3.2.3 個人情報の取扱いに注意する

自分や家族の住所、氏名、電話番号などはもちろん、家族の写真などを安易に公開するのは危険です。犯罪から身を守るため、ホームページでの個人情報の開示には十分に注意しましょう。

3.2.4 他人のプライバシーに配慮する

他人の住所、氏名、電話番号などはもちろん、他人の私生活上の事実や秘密、写真や似顔絵などを本人の許諾なくホームページで公開してはいけません。その人に嫌悪、羞恥、不快感など精神的苦痛を与え、プライバシーや肖像権の侵害となる他、場合によっては名誉、または信用の毀損となります。

3.2.5 わいせつな画像や文章を載せない

ホームページでわいせつ、売春、暴力、残虐等いわゆる「公序良俗」に反する情報を公開しないようにしましょう。

4.データ転送速度、データ容量、その他の制限

本サービス利用にあたって、規定されたデータ転送速度、データ容量、その他の制限に準拠してください。ご自分の活動が、他のユーザーのサービス利用を不適切に制限したり、抑制したり、迷惑をかけたりしていないことを常に確認してください。また、ネットワークに異常に大きな負荷がかからないように注意してください。当社のサービス、バックボーン、ネットワークノード、その他ネットワークサービスを監視する機能などへの不適切な制限、抑制、混乱、品質低下、および妨害につながるような行為は避けてください。

当社の書面による同意なしに、当社から提供されるサービスやその他の機能、またはその一部を第三者に再販売したり、供与したり、再提供したりすることはできません。当社のサービスは、個人がインターネットを使う為のものです。当社のサービスを商業目的に使うことはできません。

5.個人情報の保護

インターネットは、匿名性の世界です。したがって自分であることを証明するIDやパスワードの管理には、万全の注意を払ってください。また、あなたが自分の住所、電話番号等をインターネット上に公開することは大変危険です。一瞬のうちに、あなたの個人情報が世界中をかけめぐってしまうということを十分に認識してください。当社は、当社のユーザーに係る個人情報の保護については、当社の定めた「お客様個人情報保護方針」、「個人情報保護規程」等の他、個人情報保護に関する法令等を遵守します。また、当社が管理するユーザーから提供いただいた個人情報は、以下の場合を除き、第三者に提供されることはありません。

- ユーザーにご承諾をいただいた場合
- 当社が個人情報保護契約を締結している業務委託先、または業務提携先（販売代理店や運送会社等）に対し、業務を行う上で必要と思われる範囲の情報を開示する場合
- ユーザーによる商品の注文や有料サービスの利用等で、その代金決済のため金融機関等に個人情報を開示する必要がある場合
- 法令等に基づく要請に応じる場合

6.本ガイドライン違反が確認された場合

6.1 当社からの警告

ユーザーの皆様は、本ガイドラインを守り、インターネットコミュニティ内の良き住民となるよう常に努力してください。他のユーザーや当社サービス利用者以外のユーザーから苦情等が届いた場合、または本ガイドラインや契約約款に著しく違反した活動を行っている場合、当社は警告を出す等の適切な対応を行う場合があります。当社には、サービスやネットワークを監視する義務はありませんが、帯域幅（データ転送の状態）、サービスの使用方法、ユーザーの開設したホームページ等を随時監視する権利を保有しています。これらの活動は、サービスを円滑に運営し、違反行為を見つけ、ネットワークと当社のユーザーを守る上で必要であることをご理解ください。

6.2 警告を無視し続けた場合の措置

当社はユーザーが不適切な行為を行った場合、警告を発するなどの適切な処置を実行します。本ガイドラインや契約約款に違反した行為を続け、他のユーザーによるサービス利用や当社の営業活動を著しく妨害した場合は、当社の適切と考える対応処理を実行します。

このような対応処置には、ホームページの一時的、または永続的な削除、インターネット転送の制限、サービスの全部、または一部の一時停止、または強制解除などがありますが、これだけに限定されるわけではありません。当社には、このような対応処置を実行する義務はありません。上記の処置は例外的な処置であり、通常であれば、当社は、適切と考えられる他の合法的、または技術的な手段を実行します。

6.2.1 送信防止措置について

ユーザー（以降発信者）がホームページなどで公開している文章や画像などに対して、知的財産権、肖像権、プライバシー権、およびパブリシティー権を侵害するものである等の理由により、他のユーザーや当社サービス利用者以外のユーザーから送信防止措置の申立てが発生した場合、当社はプロバイダ責任制限法に則り、以下の手続きを行います。

- 該当の文章や画像などの自主的削除要と判断される場合は発信者へ削除要請を行います。発信者の自主的処置がなされない場合、当社にて削除措置を講じる場合がございます。
- 該当の文章や画像の自主的削除の要否が困難な場合は発信者へ削除等措置を講じて差し支えないか否かを確認します。発信者の承諾を得られた場合、または、7 日間以内の反論がない場合は該当の文章や画像の削除措置を講じます。

ユーザーホームページなどで公開している文章や画像に対して、他者の著作権を侵害するものであるという理由により、他のユーザーや当社サービス利用者以外のユーザーから送信防止処置の申立てが発生した場合、著作権の侵害であると判断される場合は、当社はプロバイダ責任制限法に則り、以下の手続きを行います。

- 当該侵害情報の送信を防止するために削除等の措置を講じます。
- 当該侵害情報の送信防止措置を講ずる旨、または講じた旨を発信者、および申出者へ通知します。

6.3 アカウント、および発信元の調査

当社は、本ガイドライン、および約款に違反したおそれのあるアカウント、および発信元を調査する権利を有しています。調査を行うケースとしては、以下のような場合があります。ただし、これだけに限定されるわけではありません。

- ウイルスメールやスパムメールなどの不正な電信メールが発信されていることが確認された場合
- 当社のユーザーや当社サービス利用者以外のユーザーが運営する電子掲示板サイトに不正な書き込みをするなどして、サイト管理者より対処依頼があった場合
- 特定のコンピュータに対して不正なアクセスが繰り返され、そのコンピュータの管理者より対処依頼があった場合
- 当社のユーザーが公開するホームページの掲載内容に不適切な文章や画像が確認された場合上記の場合、関係ユーザーや苦情を伝えてきた人々から情報を集めたり、当社のサービス利用を一時停止したり、問題のあるホームページを削除したりする場合があります。

6.3.1アカウント使用の停止に伴う措置

ユーザーがアカウントの使用を停止した場合、当社は、そのアカウントに関連するファイル、プログラム、データ、電子メールメッセージを削除する権利があります。当社が、何らかの理由でこの権利を遂行できなかった場合でも、権利を放棄したわけではありません。

7.本ガイドラインの更新

当社は本ガイドラインを事前の通知なしに随時改訂できるものとします。

平成21年4月1日

鳥取中央有線放送株式会社

■お電話の前に（トラブル時の確認）

「今まで使えていたのに急にインターネットが使えなくなった？？」
と言う場合、まずはお電話の前に以下の点をご確認ください。

症状	原因	対応
●ネットワークに繋がらない（インターネットが利用できない）	ONUの動作不良	ONUの『給電アダプタ』のコンセントを抜き差ししてください。
	中継機器※の動作不良 ※ BBルーターなどネットワーク機器	中継機器の電源のコンセントを抜き差ししてください。 ルーターのファームウェアアップデートをお試しください。
	LANケーブルの接触不良	家庭内ネットワーク内のLANケーブルを挿し直してください。

上記の点を確認していただき改善されない場合、または上記以外のトラブルの場合は下記のサポートセンターまでご連絡ください。

● インターネットの技術サポート、障害などのお問い合わせ
≪カスタマーサポートセンター≫

電話：0858-53-6200
Mail：support@torichu.co.jp
・受付日　：年中無休
・受付時間：午前 9時00分 ～ 午後 9時00分

● ご契約内容の変更・確認などのお問い合わせ
≪TCC 鳥取中央有線放送≫

（本局：琴浦町逢束806）
電話：0858-53-2565
FAX：0858-53-2791

（湯梨浜支局：湯梨浜町田後458-1）
電話：0858-35-4988
FAX：0858-35-4605

・受付日　：平日・第１、第３土曜日（祝日を除く）
・受付時間：午前 9時00分 ～ 午後 5時15分

TCC 鳥取中央有線放送株式会社
(http://www.torichu.ne.jp)